

CLAIMS

1. A method of issuing an electronic negotiable document (END) comprising: creating as data an END and storing this in a tamper-resistant document carrier, the document carrier containing a unique public-secret key pair for signing and verifying and a unique document carrier identifier; signing the unique document-carrier identifier, the END and an END identifier using the secret key of the public-secret key pair and storing the result in the document carrier.
2. A method according to Claim 1 of issuing an END, further comprising generating a time stamp representing the time of issue and storing this with the END in the tamper-resistant document carrier before the encryption step.
3. A method according to Claim 1 or 2 of issuing an END, including the step of calculating a hash value of the END and/or the time stamp value and storing this hash value instead of the full END in the tamper-resistant document carrier, before the said encryption step.
4. A method according to any preceding claim of issuing an END, in which the document carrier identifier is a device number, and the END identifier is a serial number.
5. A method according to any preceding claim of issuing an END, in which the END identifier is supplemented with data representing a water mark unique to the issuer.

6. A method according to any preceding claim of issuing an END, comprising the step of calculating a hash value of the data to be encrypted by the said secret key, in place of the full data.
7. A method according to any preceding claim of issuing an END, in which the document carrier stores a negotiability status flag indicative of whether the END stored therein is negotiable or non-negotiable, and including the step of setting the flag to "negotiable" after the result of the encryption has been stored in the document carrier.
8. A method according to any preceding claim of issuing an END, in which the document carrier includes a counter for counting a serial number, indicative of the number of times that the END has been negotiated since issue, and comprising the step of setting the counter to zero after the result of the encryption has been stored in the document carrier.
9. A tamper-resistant document carrier adapted to store an END in accordance with the method of any preceding claim, comprising read only software for controlling the steps of storing the END, encrypting the END and other data with the pre-stored secret key, and storing the result in a memory.
10. A document carrier according to Claim 9, in which the memory includes a negotiability status flag capable of being set either to "negotiable" or to "non-negotiable".
11. A document carrier according to Claim 9 or 10, in which the memory includes a counter for storing a serial

number representative of the number of times the END has been negotiated.

12. A method of negotiating an END between a seller and a buyer each possessing a tamper-resistant document carrier having its own public-secret key pair, in which the END is stored in the seller's document carrier in the form of END data, and the signature generated by the secret signing-key of a document carrier of the issuer of the END, together with a negotiability status flag indicative of whether the END is currently negotiable from the document carrier on which it is stored, comprising establishing mutual recognition between the seller and buyer using a predetermined protocol between the respective document carriers, verifying in the seller's document carrier that the negotiability status flag is "negotiable" and aborting the negotiation if not, sending the public encryption key of the buyer's document carrier to the seller's document carrier, and using it to encrypt the message comprising the END together with the negotiability status flag, sending that encrypted message to the buyer, decrypting that message using the buyer's secret decryption key, and setting the negotiability status flag for that END of the buyer's and seller's document carriers respectively to "non-negotiable" and "negotiable".

13. A method of negotiating an END between a seller and a buyer each possessing a tamper-resistant document carrier having its own public secret key pair, in which the END is stored in the seller's document carrier in the form of END data, and the signature generated by the secret signing key of a document carrier of the issuer of the END, together with a serial number counter

indicative of the number of times that the END has been negotiated since issue, comprising establishing mutual recognition between seller and buyer using a predetermined protocol between their respective document carriers, verifying in the seller's document carrier that the END, if it has been stored previously in that document carrier, has a different counter value this time and is therefore negotiable, but aborting the negotiation if it is not negotiable, sending the public encryption key of the buyer's document carrier to the seller's document carrier, and using it to encrypt the message comprising the END together with the counter, sending that encrypted message to the buyer, decrypting that message using the buyer's secret decryption key, and incrementing the counter by one.

14. A method according to Claim 12 or 13, in which each document carrier is installed originally with a certificate comprising a digital signature of its unique identifier and of its public key.

15. A method according to Claim 14, in which the certificate unique to the document carrier on which the END was originally issued is stored with the END in the seller's document carrier.

16. A method according to Claim 14 or 15, in which the certificate of the buyer's document carrier is sent to the seller's document carrier in which it is authenticated and the negotiation is aborted if authentication fails.

17. A method according to any of Claims 12 to 16, in which the buyer's document carrier, after decrypting the

message using its secret key, verifies the signature of the issuer on the END, and informs the issuer in the event that authentication fails.

18. A method according to any of Claims 1 to 8 of issuing an END on a document-carrier followed by a method of negotiating the END as claimed in any of Claims 12 to 17.

19. A method according to Claim 18 as appendant to Claim 2, in which the buyer's document carrier, after decrypting the message with its secret key, verifies that the END is still valid by taking its time stamp, and, if it has expired, informs the issuer of this, and aborts the negotiation before implementing the counter or setting the negotiation status flag.

20. A method according to any of Claims 12 to 19 including recovering the negotiation of an END which has previously broken down, by providing the buyer's document-carrier with the necessary secret key which has been reproduced by the issuer or by a trusted third party.

21. A method according to any of Claims 12 to 19 including recovering an END lost from a primary document-carrier, by activating a back-up document-carrier which has previously been provided with back-up data reproduced from the primary document-carrier.

22. A method according to Claim 20 or 21, comprising inhibiting the recovery until the expiry of the predetermined period of validity of the END.

23. A method of negotiating an END, sold by a seller to a buyer, in which the buyer splits the END electronically into two or more parts and then negotiates those parts separately to one or more further buyers.

24. A method according to Claim 23, in which each part is subjected to the digital signature of the said buyer's document carrier which effects the splitting.

Add
A1